Secure Real-Time Information Sharing in Artificial Intelligence Driven Freight Forwarding for Green Supply Chains

Apeksha Garg[1,*], Sudha Vemaraju[2]

[1]Research Scholar, GITAM School of Business, GITAM University (Deemed to Be University) - Hyderabad, India

[2]Associate Professor, GITAM School of Business, GITAM University (Deemed to Be University) - Hyderabad, India

Emails: apeksha.k.garg@gmail.com; svemaraj@gitam.edu

Abstract

The integration of artificial intelligence (AI) and real-time information sharing is transforming the freight forwarding industry, enabling more sustainable and efficient green supply chains. However, the increasing reliance on interconnected systems raises significant cybersecurity challenges, particularly regarding secure data exchange and protection of sensitive information. This paper explores the critical role of cryptographic models and secure communication protocols in safeguarding real-time data sharing among AI-driven logistics networks. We analyze key security challenges faced by IoT-enabled freight systems and propose robust encryption and key distribution strategies to ensure confidentiality, integrity, and resilience. Our findings highlight the importance of secure information management in advancing sustainable, cyber-resilient supply chains that support environmental goals while maintaining operational efficiency.

Keywords: Artificial intelligence; Information sharing; Green logistics management; Sustainability; Freight forwarding industry; Green supply chain management

1. Introduction

The logistics along with freight forwarding industry exists in a crucial position between sustainability and innovative progress in times of climate change and environmental deterioration and rapid digital developments. Supply chains operate as essential competitive areas because environmental responsibility meets with operational capability [1]. Supply chain revolution strives to develop networks, which lower pollution and ensure the maximum use of resources with minimal waste production. The essential part of international trade known as freight forwarding holds a fundamental position throughout this system. The challenge becomes difficult to overcome as global trade grows while customers want rapid shipment handling and product tracking records simultaneously. Secure real-time information sharing together with Artificial Intelligence (AI) presents an effective response method for multiple challenges faced by the industry [2].

The strategic management process of transporting freight via multiple shipping methods crosses through different territorial areas to reach its destination is known as freight forwarding. The traditional forwarding approach depends on manually coordinated processes along with numerous disconnected communication methods that use outdated systems [3]. The inefficient processes result in two negative impacts because they slow down system agility while simultaneously creating avoidable environmental strains from excessive fuel consumption and wasted trips and degraded container loading efficiency [4]. The deployment of predictive analytical technologies in automated systems leads organizations to optimize their operational processes in freight forwarding activities. The global freight transportation sector undergoes revolutionary changes because Artificial Intelligence systems now conduct demand prediction service alongside autonomous vehicle arrangement and route management and system anomaly identification tasks. The maximum potential of these technological solutions becomes accessible through secure data sharing and real-time information exchange between the complete logistics network [5].

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

All parties involved in supply chain operations—the shippers together with freight forwarders and carriers and customs agents and customers—can obtain precise current data through real-time information sharing systems. The system provides information about delivery status combined with geographical tracking data as well as estimated delivery durations and any delay updates and environmental performance analysis that reveals carbon footprint details. Prompt secure data distribution leads to efficient proactive choice making which minimizes system inefficiency to deliver better overall system performance [6]. The supply chain becomes better at managing assets through time-sensitive information, which enables route adjustments for fuel reduction together with optimized load assembly and dynamic scheduling of activities to reduce vehicle idle time and cut emission levels. Data stream purposes create essential security and privacy along with trust-related problems because of real-time information transmission. Operational freight forwarding manages crucial business data and logistics trade secrets together with exposing endpoints that might include IoT devices and mobile platforms to security risks. To avoid data breaches and cyberattacks as well as misuse of information the establishment of secure transmission combined with proper access control becomes essential [7].

The security situation becomes more challenging because of AI implementation. AI systems depend on extensive datasets yet their operation based on continuous data inputs and external information generates novel ways for cyber threats that include data poisoning and adversarial attacks. Through automatic freight forwarding tasks AI systems make it possible for malicious data and compromised inputs to produce actual errors such as wrong delivery routes and unapproved cargo handling [8]. Desirable secure architecture together with data sharing protocols need development to include encryption along with authentication features and access controls in addition to data integrity protection measures. Freight forwarding operations require standardized policies for data governance to ensure interoperability between stakeholders who come from different organizations and jurisdictions.

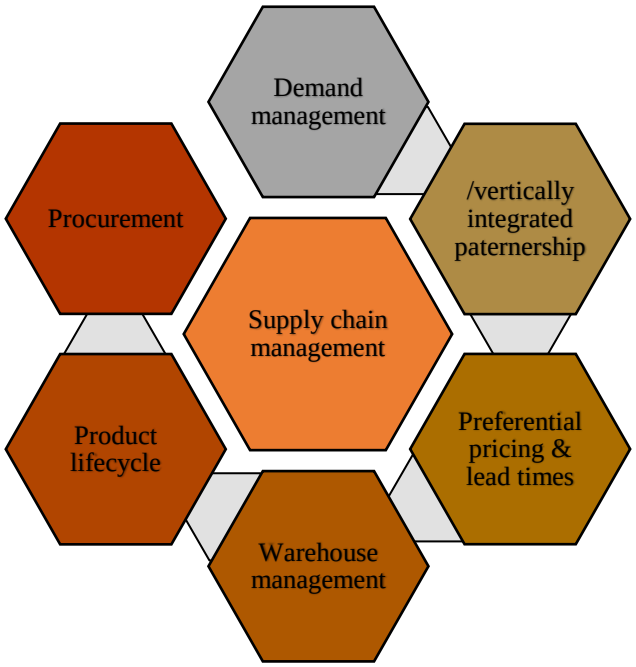

Figure 1. Key Components of Supply Chain Management

The Figure 1 demonstrates how supply chain management works by showing the vital components which start with demand management and continue through procurement followed by transportation and inventory control and warehouse management before finishing with strategic partnerships to achieve efficient product delivery to end consumers.

Blockchain together with distributed ledger technologies provide effective solutions for protective information sharing within these domains [9]. Through robust data protection and consensus protocols and clear record documentation, blockchain creates trustworthy networks for business partners who normally operate without existing framework connections. The implementation of smart contracts enables automated execution of both compliance checks together with payments processing and data validation tasks, which removes the requirement for human intermediaries along with manual monitoring processes [10]. Capitalize on the need to examine the

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

blockchain implementation issues related to scalability, latency, and energy requirements during real-time operations in freight management. Blockchain technology exists without solving all issues because its effective deployment requires deliberate integration with AI systems and cloud platforms as well as edge computing infrastructures for operational efficiency and global data security standards including ISO 28005 and EU GDPR.

Secure real-time analytics get their operational foundation from edge and cloud computing systems. The data processing abilities of GPS trackers, telematics units and smart sensors on vehicles and containers located at edge points ensure reduced delays and decreased data transmission requirements. The cloud offers businesses broad capabilities to run flexible AI training operations with worldwide data collection features and advanced analytic capabilities [11]. Real-time responsiveness can be achieved through a dual-edge-cloud computing system, which keeps central control functions and maintains complete oversight. Such integrations increase the vulnerability points that need robust security measures and identity management systems and zero-trust architectures to protect against potential attacks.

Environmental performance standards together with industrial regulations show progress because of the merging AI systems with logistics sectors and sustainability demands. Governments together with international bodies create incentives for green logistics by mandating carbon reports and emission restrictions as well as environmental data publication [12]. The frameworks require comprehensive and expedited data disclosure for compliance purposes, which strengthens the need to establish safe real-time information sharing methods. PSR and ESG criteria pressure logistics providers to reveal sustainable operational procedures as well as enhance operational transparency. Organizations combining AI-driven freight forwarding with secure data practices become able to fulfill regulatory requirements and position themselves as leading environmentally aware and technological frontrunners in the market [13].

Secure real-time information sharing that uses AI within freight forwarding operations produces effects that reach beyond efficient operations and regulatory fulfillment. The supply chain collaboration becomes better together with customer satisfaction improvement and quicker carbon-neutral logistics adoption. Adaptable supply chains for environmental emergencies as well as geopolitical events and pandemic scenarios can be built when data silos are eliminated and trust-building abilities are implemented [14]. Secure data sharing systems will assume the critical role of allowing AI modules to scale up their learning ability as capabilities advance more rapidly.

Real-time secure information sharing functions as the base requirement that AI-driven freight forwarding needs to establish successful operations within green supply chains. Such technology serves as the connection between innovation and stewardship, which establishes sustainable and intelligent logistics operations. The pathway to success contains substantial technical issues yet multiple chances to advance exist [15]. A secure freight forwarding process built on trusted data systems throughout all delivery operations will drive the industry toward its sustainable business goals.

2. Related Work

Multiple dimensions exist in the research of Artificial Intelligence (AI) applications to freight forwarding and supply chain logistics because scientists want to understand how to securely share real-time data for developing sustainable green logistics networks [16]. The subsequent part provides details about current methods concerning data protection alongside Artificial Intelligence applications within logistics services as well as sustainability considerations for supply chain operations.

2.1 AI-Based Optimization in Freight Forwarding

AI-driven freight forwarding operates as a technology revolution, which enables traditional logistics to adopt both self-directed and predictive operational systems. Machine learning together with reinforcement learning and deep learning serves as common methods for enhancing transportation route optimization as well as demand estimation along with real-time supply chain adjustments [17]. Applications of neural networks to multifaceted navigation and immediate traffic forecasting have significantly improved delivery while having a smaller impact on the environment due to decreased idle time and fuel use.

Research on supply chain coordination utilizes intelligent agents as well as AI planning algorithms to help different supply chain stakeholder's work together by enabling cooperative decision-making in transportation planning activities [18]. AI systems need real-time access to diverse data sources for their operations that in turn creates a need for reliable and secure data-sharing methods.

2.2 Secure Data Sharing Through Blockchain Integration

Blockchain technology applications in logistics have become important because they provide dependable data sharing solutions. Blockchain-based platforms operate with tamper-proof ledgers that document every supply chain occurrence, which makes them exceptional for shipping state tracking as well as delivery authentication along with environmental requirements verification.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

Industrial organizations prefer permissioned blockchain networks from Hyperledger Fabric and Quorum platforms because these systems offer scalability features together with data privacy controls [19-21]. The systems permit authorized stakeholders to view data while preventing unauthorized access to sensitive business information during collaborative work activities. The implementation of smart contracts improves document testing as well as customs process execution and payment processes through automation, which results in both improved speed and enhanced transparency. The research community has discovered multiple hurdles to secure data exchange benefits through blockchain technology such as system latency issues in real-time operations and high-energy requirements of public blockchain networks and integration obstacles with existing legacy IT infrastructure.

2.3 Edge and Cloud Computing for Real-Time Responsiveness

Real-time freight forwarding systems need solutions with hybrid architectures of edge along with cloud computing because they help handle latency requirements and scalability needs [22]. Phants running at edge locations allow local data processing either on devices or close to their source for applications including GPS-based tracking needs together with in-transit environmental monitoring and real-time anomaly detection. The centralized capabilities of cloud computing allow users to run AI training models and execute big data processing and manage international logistics information databases.

Edge devices employ a multi-layered structure to acquire data, which they process into relevant information to transmit through the cloud platform for analytical purposes. The method reduces data exchange costs and speed up response times while distributing only useful data for upstream sharing [23-25]. The decentralized processing system creates new obstacles concerning device synchronization together with secure data protocols and network access management.

The proposed solutions for these problems include lightweight encryption schemes as well as secure multiparty computation (SMC) and federated learning frameworks that maintain data security together with computational efficiency.

2.4 Interoperability and Standardization of Logistics Data

Seamless information exchange in global logistics networks remains hindered because different stakeholders lack a standardized way to exchange data and use interoperable system platforms. Multiple academic investigations demonstrate the segregated nature of the digital network systems, which freight stakeholders like carriers maintain along with customs firms and warehousing management systems and third-party logistics entities. Industry-led initiatives have launched projects to create shared communication specifications (such as Electronic Data Interchange and UN/EDIFACT as well as ISO 28005) which enable data exchange between systems [26].

Researchers in this field explore middleware systems with integration elements that create connections between disparate systems by doing format translation and real-time access right management. The access control systems within these platforms rely on RBAC and ABAC models to allow users reach only data associated with their operational duties. Research on Application Programming Interfaces (APIs) investigates how these technologies empower real-time data combination but focuses especially on how secure API gateways protect data from breaches and unauthorized entry [27].

2.5 AI-Enhanced Cybersecurity for Logistics Platforms

AI defends real-time logistics systems through its application as a security measure for heightened cybersecurity. Data anomaly detection methods check for abnormal patterns, which signal potential cyberattacks together with data manipulation or unauthorized internal activities [28]. Research has developed intrustion detection systems (IDS) based on machine learning to learn normal network traffic patterns while detecting up-to-date anomalies.

Deep learning model components that include autoencoders and recurrent neural networks (RNNs) function for detecting upcoming security breaches so administrators can protect vulnerable points before they are exploited [29]. These monitoring tools show particular value for logistics system operation since they detect threats among multiple constantly communicating IoT devices beyond human observation capabilities.

AI techniques for privacy preservation have become more popular because they enable the analysis of distributed sensitive logistics data through differential privacy and homomorphic encryption and federated learning approaches.

2.6 Sustainable Logistics and Green AI Models

Research about sustainability together with artificial intelligence in supply chains has risen to a critical state of urgency. AI optimization technology operating in real-time demonstrates capabilities to decrease greenhouse gas emissions through its improvement of delivery routes and its elimination of unnecessary driving and better

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

management of shipment loading weights [30]. Experts are now examining the carbon emissions of AI technology since its training steps and its data center facilities require significant power consumption.

The software development field focuses on building "Green AI" models, which focus on computer power efficiency alongside data responsibility utilization [31]. These computational models achieve performance-of-environment harmony through the implementation of approximation algorithms and both pruning techniques and energy-aware scheduling. Real-time tracking of environmental KPIs occurs through several logistics solutions as these platforms monitor CO_2 emission rates per delivery or per ton-kilometer. The KPIs provide input to automated systems that improve operational strategies to achieve sustainability targets.

2.7 Collaborative Logistics Platforms and Data Trust Models

Despite the limited adoption of collaborative logistics platforms researchers seek to create environments, which enable various supply chain participants to exchange data securely. These digital platforms break away from traditional data protection approaches through a system that provides access to shared transportation resources, optimized route solutions, and jointly managed inventory operations.

Different trust models exist to solve trust-related problems that emerge from multi-stakeholder frameworks [30]. The current data security standards comprise three elements that are cryptographic trust anchors and zero-knowledge proofs together with decentralized identity management systems. Data escrow services along with auditable logs serve as methods to validate that all parties maintain compliance with their agreed data-sharing policies according to certain approaches [32].

Such collaborative platforms succeed as platforms when they establish precise data governance frameworks in addition to legal agreements and economic incentives that motivate participants to behave honestly [32].

Research currently available provides essential guidelines for constructing secure communication platforms for AI-based freight forwarding systems that operate in real time. The fields of blockchain and sustainable logistics together with artificial intelligence optimization and edge computing have advanced but the necessary integration of systems and work together remains limited. Research should focus on generating complete frameworks that unite security protocols with sustainable information sharing systems for creating advanced environmentally friendly supply networks.

3. Objectives of the Research

The research conducts studies to develop and evaluate an information-sharing framework dedicated to securing real-time operations, which increase AI-driven freight forwarding system efficiency while sustaining operations and strengthening cyber-resilience. Advanced cryptographic security models linked to intelligent data processing alongside secure communication protocols build the core of this research since they fight against rising cybersecurity threats in logistics networks. The research protects IoT-enabled platform data transmissions of sensitive freight information by maintaining confidentiality and integrity and authenticity alongside operation speed. The framework actively assists green supply chain activities through its capability to provide wise decisions and optimization of delivery routes and manageable environmentally friendly logistics activities. The proposed research implements an algorithm that integrates secure transmission alterations with encryption together with anomalous detection system and key management for real-time logistics coordination. Simulation with analysis techniques and case validation during this research demonstrates the relationship between secure information sharing with sustainability goals, environmental responsibility, and supply chain transparency targets in global freight networks.

4. Motivation of the Research

The freight forwarding industry experiences a digital revolution because of artificial intelligence (AI), real-time data sharing, and Internet of Things (IoT) technologies in this present interconnected world. These technologies give enterprises significant possibilities to enhance their operations through improved efficiency and lower carbon footprint and better supply chain sustainability. Logistics systems that incorporate intensified data management and AI systems expose themselves to a greater number of cyber threats. Conservative security measures applied to current supply chain infrastructures expose organizational data and operations to vulnerabilities that threaten privacy and continuous operation and faith from stakeholders.

The research has been launched to address the essential need of connecting sustainability targets with cybersecurity measures in freight logistics. The complete benefits of AI-driven real-time data systems for efficiency and environmental benefits remain locked until secure communication frameworks achieve resilience in operations. Secure operations under a trusted digital environment can be achieved through this research based on its advanced cryptographic methods with secure protocols alongside intelligent monitoring systems. The research motivates academic and industry leaders because they recognize achieving green, intelligent and secure logistics systems as a fundamental strategic need for global trade combined with environmental protection.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

5. Proposed Work

This study presents an integrated solution, which combines cryptographic technology with artificial intelligence to accomplish dual sustainability and cybersecurity goals in AI-driven freight forwarding systems. Real-time data flows through IoT devices within green supply chains increase the substantial dangers of cyber threats and data breaches. A strong security system must be implemented to protect data sharing processes due to the technological complexity that demands efficient AI systems remain functional. The optimization of secure sustainable logistics control happens through combining multi-party computation and specialized cryptographic protocols, which work for IoT environments and machine learning systems to secure data while ensuring performance within IoT systems. The system obtains extended resistance through quantum-resistant algorithms together with blockchain-based logging mechanisms that also guarantee improved tracking capabilities.

The figure 2 illustrates the flow of the proposed approach.

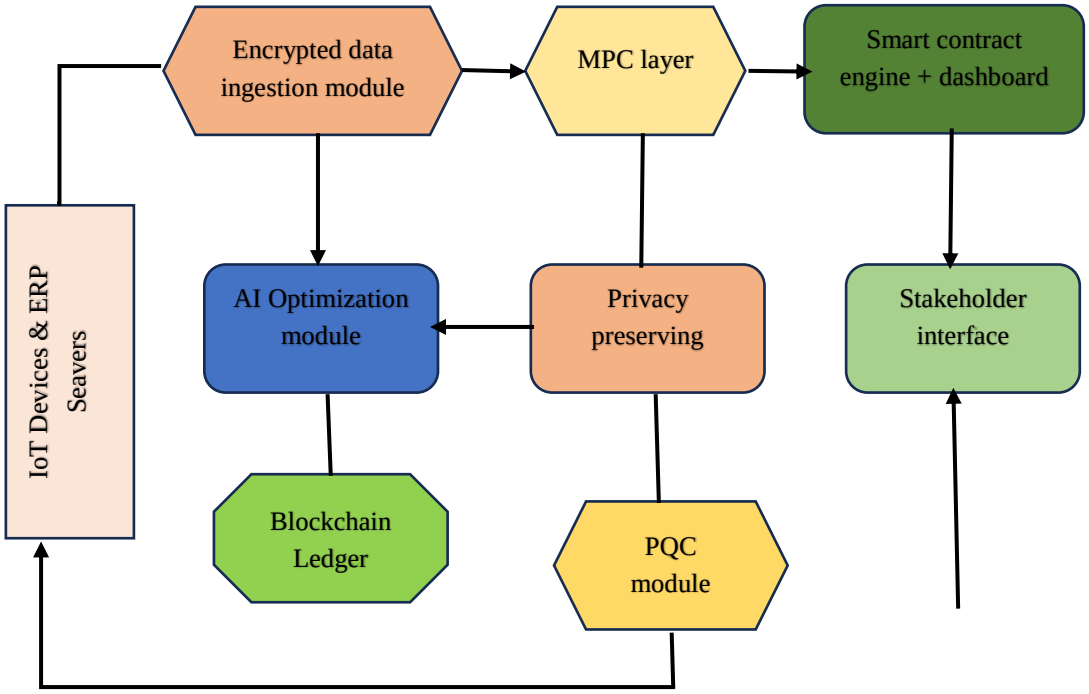

Figure 2. Secure Ai-Driven Logistics framework for green supply chains

5.1 AI-Driven Freight Optimization Engine

Artificial intelligence drives the decision-making mechanism, which operates as the essential part of real-time logistics optimization through the AI-Driven Freight Optimization Engine. The engine receives uninterrupted sensor and operational data streams to produce cost-effective sustainable routing schedules that optimize results. Supervised and reinforcement learning techniques operate within this module to process vehicle telemetry together with environmental sensors and warehouse status along with customer demand information. During time t the system accepts input through a vector $x_t \in \mathbb{R}^d$ that contains d features including distance and fuel cost combined with load weight and weather condition measurements.

Through parameter θ the AI model develops an approximation function $f_\theta: \mathbb{R}^d \to \mathbb{R}^k$ that outputs k result parameters which may include delivery time and route priority along with emission scores. A neural network or ensemble model determines the weights θ that parameterize the model. The output of predictive decisions appears as:

$$\hat{y}_t = f_\theta(x_t) \quad (1)$$

The model requires a combined loss function as part of its training process to fulfil both operational and environmental targets.

$$\mathcal{L} = \alpha \cdot \| \hat{y}_t - y_t \|^2 + \beta \cdot E(\hat{y}_t) \quad (2)$$

where, $\|\cdot\|^2$ = mean squared error, $E(\hat{y}_t)$ = cost or emissions function, α and β = balancing weights.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

The agent in dynamic environments uses reinforcement learning to accept state information s_t and perform action a_t to achieve maximum expected rewards.

$$\pi^* = \underset{\pi}{\text{argmax}}\mathbb{E}[\sum_{t=0}^{\infty}\gamma^t R(s_t, a_t)] \quad (3)$$

Through the optimization of policy π^* system decision-making processes seek sustainable operational results while also minimizing delays along with emissions and costs in real-time operation.

5.2 Cryptographic Framework for Secure Communication

The AI-driven freight forwarding system relies on a combined asymmetric and symmetric encryption framework to establish both fast data transmission and protected key exchange for constant data exchange. The dual-tiered encryption solution protects distributed logistics data by maintaining confidentiality along with integrity and blockage of both eavesdropping attempts and unauthorized modifications.

Symmetric Encryption:

The system protects high-speed data using AES-GCM (Advanced Encryption Standard in Galois/Counter Mode) because of its popularity for resource-limited IoT devices. Using a secret key K together with message data P and nonce N leads to the production of ciphertext C and authentication tag T by the encryption process.

$$(C, T) = \text{AES-GCM}_K(P, N, A) \quad (4)$$

Additional authenticated data (A) represents message headers and the message verification occurs through tag (T). Decryption checks that:

$$P = \text{AES-GCM\_Decrypt}_K(C, N, A, T) \quad (5)$$

An invalid authentication tag results in cryptographic failure because it ensures data integrity was not compromised.

Asymmetric Key Exchange:

ECDH provides the platform with Elliptic Curve Diffie-Hellman (ECDH) to securely create the shared key K. The private keys (a or b) correspond to each party but they use a base point G from an elliptic curve E to calculate their public keys.

$$P_A = aG \quad , \quad P_B = bG \quad (6)$$

The shared secret derives from the following calculation:

$$S = aP_B = abG = bP_A \quad (7)$$

The symmetric keys emerge from S through a Key Derivation Function (KDF).

$$K = \text{KDF}(S) \quad (8)$$

The arrangement combines encryption with keyless communication to stop intermediary attacks throughout sessions. Both AES-GCM and ECDH create an efficient secure infrastructure to protect real-time logistics data sharing in AI-dependent IoT systems.

5.3 Privacy-Preserving Multi-Party Computation (SMPC)

The platform of Privacy-Preserving Multi-Party Computation (SMPC) allows multiple parties to run joint functions on private inputs without revealing their individual data among the participants. The joint optimization of logistics decisions becomes possible through SMPC when different entities (such as carriers and shippers and customers) need to work together for route planning and load distribution without exchanging confidential information.

Secret Sharing Scheme: Protection at SMPC demands Secret Sharing that separates a secret s into multiple shares $s_1, s_2, \ldots, s_n$ distributed to individual parties. In t-threshold secret sharing the secret s is encoded through a degree t−1 polynomial f(x).

$$f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \quad (9)$$

The share given to party i equals the evaluation of function f for argument i. The reconstruction of lost secrets requires at least t of the available distributed shares. Each share distribution process prevents solitary parties from understanding the secret information.

Lagrange Interpolation for Reconstruction: Enough available shares allow Lagrange interpolation to reconstruct the original secret s. A reconstruction of the secret s occurs through this process: $(i_1, s_{i_1}), (i_2, s_{i_2}), \ldots, (i_t, s_{i_t})$.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

$$s = \sum_{j=1}^{t} s_{i_j} \cdot \prod_{\substack{1 \le m \le t \\ m \ne j}} \frac{i_m}{i_m - i_j} \quad (10)$$

The shares-based reconstruction procedure reveals ss accurately without compromising the individual values.

Secure Computation on Shared Data: Splitting a secret allows parties to conduct computations through their shares while keeping the underlying data germs hidden. The computation of $\sum_{i=1}^{n} x_i$ requires summing the private inputs $x_1, x_2, \ldots, x_n$ through an operation on the shares $s_1, s_2, \ldots, s_n$ which looks as follows:

$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} \text{Reconstruct}\,(s_i) \quad (11)$$

The result becomes available to every participating party through this computational procedure, which maintains individual input secret. Secure decision-making processes through SMPC allow different stakeholders to work together without learning what other participants keep private within logistics networks.

5.4 Quantum-Resistant Key Distribution

RSA and ECC (Elliptic Curve Cryptography) face security risks due to quantum computation because Shor's algorithm along with other quantum algorithms succeed in solving discrete logarithms and factorizing large numbers. Modern cryptographic keys need replacement because quantum-resistant key distribution methods have become necessary. The security of lattice problems combined with additional hard problems in cryptographic algorithms ensures protection against quantum-computing threats.

Post-Quantum Cryptographic Protocols: The key distribution protocol based on lattice-based cryptography represents a promising solution because of security-enhancing mechanisms such as Kyber, which works as a quantum-resistant key encapsulation mechanism (KEM). The security foundation for Kyber cryptography depends on the difficult Module Learning with Errors (MLWE) problem that quantum computers along with classical computers have great challenges solving.

During Kyber key exchange, the participating entities create both public keys and private keys. The private key of party A is denoted as AA while its public key equivalent is named P_A and this pair is produced through a polynomial-based function. The process is as follows:

Key Generation: Private Key selection occurs randomly through the choice of $a \in \mathbb{Z}_p$ before the public key P_A derives from it using the polynomial map $f_a(x)$ which functions on lattice points.

$$P_A = f_a(x) \quad (12)$$

Key Encapsulation: In the key encapsulation process Party B generates random value r to produce ciphertext ct_B containing the shared secret.

$$\text{ct}_B = \text{Kyber.Encaps}(P_A, r) \quad (13)$$

The ciphertext ct_B enables A to retrieve the shared secret while maintaining complete secrecy about its private key information.

Key Decapsulation: The ciphertext ct_B enables Party A to generate the shared secret K through the utilization of its private key a.

$$K = \text{Kyber.Decaps}(P_A, \text{ct}_B) \quad (14)$$

The scheme produces a key K through the quantum-resistant process that enables symmetric encryption with AES as an example.

Quantum Security Guarantee: Quantum machines find it computationally difficult to break the security provided by the Kyber and other lattice-based schemes. LWE represents the fundamental problem that drives these algorithms because quantum specialists have not discovered efficient solutions to this problem, which ensures extended security capabilities through the post-quantum period.

5.5 Blockchain-Enabled Audit and Traceability

The blockchain system creates an untampered distributed database structure that enables clear monitoring while making transactions accessible to every supply chain member. The audit and tracking of important logistics activities by AI-driven freight forwarding services becomes feasible through blockchain implementation which produces decentralized records of all transaction operations including cargo loading and customs clearance and delivery processes.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

Event Hashing and Blockchain Integration: Event E_i includes package shipments and route updates that generate unique event fingerprints $H(E_i)$ by applying secure hash function H (SHA-256). The blockchain records the hash value $H(E_i)$ that has been obtained through the event hashing process.

$$H(E_i) = \text{SHA256}(E_i) \quad (15)$$

The hash function provides cryptographic evidence that verifies event authenticity because it locks the recorded data into an unalterable state. The hash value from the last event connects to the present event to produce a block chain structure.

Block Construction: The blockchain structure contains two parts, which include the block header section, and the transaction set known as events i. Each new block header consists of the last block hash $H(B_{i-1})$, the present block hash $H(B_i)$ and the timestamp Time_i:

$$B_i = \{H(B_{i-1}), T_i, \text{Time}_i, H(B_i)\} \quad (16)$$

Through blockchain technology the system generates an unalterable database structure called B_i that joins all cryptographic information while preserving every transaction event permanently.

Consensus Mechanism: Every blockchain system needs an agreement method like Proof of Work (PoW) or Practical Byzantine Fault Tolerance (PBFT) so that its ledger state receives approval and validation. The system permits everyone including attackers to maintain identical cryptographic observations about system transactions. The mathematical formula to describe consensus function emerges as:

$$\text{Consensus}(\mathcal{L}_i, \mathcal{L}_{i+1}, \dots) = \text{Valid}(B_i) \quad (17)$$

At each time step $\mathcal{L}_i$ shows the ledger that the system must agree upon for validation.

Audit and Traceability: Security logs of blockchain events provide complete asset tracking capabilities because they maintain a documented trail that extends back to their initial source. When querying the blockchain for audit purposes users gain access to the comprehensive record of events, which proves the status and timestamp accuracy of every logistics operation. Every blockchain system provides complete visibility through its transparent features to conduct audits at any time thus requiring zero authorization from a centralized institution.

5.6 Integrated Workflow for Secure AI-Driven Logistics

Secure AI-Driven Logistics operation efficiency boosts through the Integrated Workflow, which links secure data sharing methods and blockchain systems with AI to enhance supply chain sustainability as well as security protection. The workflow connects multiple components into an integrated system which enables stakeholders to securely share data with real-time processing while making predictions and conducting joint efforts. This system protects data integrity along with stakeholder privacy.

Data Collection and Real-Time Monitoring

Multiple sensors linked to the Internet of Things (IoT) provide data collection as the initial process within the integrated workflow. The sensors track essential variables including temperature and location and load status and humidity reading in real-time. The AI system processes data after it receives the information sent from various monitoring points.

The data points undergo simultaneous blockchain-based recording for achieving trustworthy and tamper-proof storage. The data securing process includes hash functions that produce cryptographic fingerprints that are added to distributed ledgers thus enabling complete visibility and tracking.

The data point produced by an IoT sensor at time t_i is denoted as D_i.

$$D_i = \{\text{Location}_i, \text{Temperature}_i, \text{Load}_i, \text{Timestamp}_i\} \quad (18)$$

After data processing takes place blockchain adds this data while generating a special hash known as $H(D_i)$.

$$H(D_i) = \text{SHA256}(D_i) \quad (19)$$

The hash functions create an unalterable record that maintains the block data on the blockchain.

AI-Driven Decision Making

AI algorithms immediately examine collected data, which has been verified to make optimal decisions. The model uses reinforcement learning together with supervised learning or neural network algorithms to make critical routing decisions as well as inventory management and forecasting predictions.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

The AI system utilizes $D_t = \{D_1, D_2, \ldots, D_n\}$ real-time data stream to create predictive analyses through its processing capabilities. The optimized decision output received by the system is denoted as y_t which means both route optimization and delivery scheduling among other variants.

$$y_t = f_\theta(D_t) \quad (20)$$

The AI model f_θ operates with weights θ that control its functionality. The function accepts current data D_t through its input to produce output y_t that represents the optimized action.

The AI system receives feedback and learns from previous decisions that allows its model to adapt automatically in response to traffic variations and changes in customer demand together with environmental conditions.

Secure Communication and Cryptographic Protocols

Multiple logistics parties need secure communication channels, which protect confidential information and avoid data theft so they can maintain privacy. The exchange of secure data implements AES-GCM for symmetric encryption along with ECDH (Elliptic Curve Diffie-Hellman) protocols for key exchange protocols.

The secure key exchange establishes K as the shared key and M represents the message, which must be transmitted. The encryption process through AES-GCM generates encryption output C and authentication tag T from the original message.

$$(C, T) = \text{AES-GCM}_K(M) \quad (21)$$

The received message is decrypted before authenticity checking takes place through the authentication tag evaluation.

$$M = \text{AES-GCM\_Decrypt}_K(C, T) \quad (22)$$

The method guarantees protected exchanged messages that stakeholders including carriers, shippers and customers can verify with complete authorization and confidentiality.

Blockchain-Enabled Audit and Traceability

The system integrates Blockchain to establish complete tractability, which allows inspection of every recorded action through an auditable system. All route selects decisions and goods loading activities are written to this blockchain that builds an unalterable record of the supply chain operations.

The scenario begins with a delivery event-taking place. The delivery event E_t contains specific details about the transported items together with departure time and predicted arrival time and traveling path information. This event is hashed:

$$H(E_t) = \text{SHA256}(E_t) \quad (23)$$

The blockchain process creates new blocks, which include both preceding event hashes and the current addition to the blockchain chain. The blockchain construction enables every stakeholder in the supply chain to examine and confirm successive events that ensures open visibility while stopping criminal activities. Blockchain integrity is protected by consensus mechanisms consisting of Proof of Work (POW) and Practical Byzantine Fault Tolerance (PBFT that stop unauthorized modifications to the ledger.

Privacy-Preserving Multi-Party Computation (SMPC)

The Privacy-Preserving Multi-Party Computation (SMPC) methods ensure security for sensitive information including pricing details and customer data. SMPC enables different parties to perform joint calculation of functions across their confidential inputs without disclosing their data sets. The freight forwarding system demands stakeholders to calculate delivery costs from private price models while preventing model exposure between parties.

Two entities A and B maintain different private inputs designated as x_A and x_B respectively. The function needs to compute $f(x_A, x_B)$. When utilizing SMPC techniques the parties manage to execute the $f(x_A, x_B)$ calculation while maintaining complete privacy regarding their respective inputs. After the compute procedures end, the final answer appears.

$$f(x_A, x_B) = \text{SMPC}(\{x_A, x_B\}) \quad (24)$$

Through this approach, both parties can work together without revealing their confidential data.

Secure Key Distribution and Management

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

Two quantum-resistant key distribution methods such as lattice-based cryptography or Quantum Key Distribution (QKD) create end-to-end security for logistics systems through secure key exchange between parties. Even with the future trend of quantum computing these cryptographic methods protect the security of encryption keys.

The integrated workflow for secure AI-driven logistics implements a complete system through AI decision-making capabilities and blockchain traceability features along with cryptographic security measures and confounders to protect confidential information exchange. Through these measures, the supply chain system achieves optimized and secure automated operations and full transparency.

6. RESULTS

Secure AI-driven logistics operations showcase maximum effectiveness from the implementation of AI together with blockchain and cryptography and privacy-protecting techniques. The combination of predictive decision-making with AI generates real-time optimization and blockchain enables unalterable traceability as a security measure for the system and private information management. The security profile of the system reaches increased levels through cryptographic protocols and quantum-resistant key distribution methods. The study demonstrates the development potential of a sustainable logistics network that achieves operational efficiency and supply chain demands as well as data protection and resilience.

Time-to-Delivery (TTD) measures the complete duration required for shipment moves from their initial creation through to destination delivery. It can be calculated as:

$$\text{TTD} = \frac{\text{Total Delivery Time}}{\text{Number of Shipments}} \quad (25)$$

The computation of Cost-per-Unit (CPU) determines price based on delivering a single unit product such as per ton or per package. It is calculated as:

$$\text{CPU} = \frac{\text{Total Logistics Cost}}{\text{Total Units Delivered}} \quad (26)$$

The Data Integrity (DI) measure represents the total number of messages that successfully complete their integrity test using cryptographic hash functions.

$$\text{DI} = \frac{\text{Number of Verified Messages}}{\text{Total Messages Transmitted}} \quad (27)$$

A system that exhibits scalability shows its capability to maintain consistent performance levels when processing rising workloads or enlarging capacity parameters. Logistics systems need scalability to manage rising network data volumes, higher shipments and expanding networks that include new stakeholders.

The Privacy Leakage Rate **(**PLR) parameter helps evaluate SMPC's privacy security through its ability to measure the amount of confidential data exposed during collaborative statistics processing. This is calculated as:

$$\text{PLR} = \frac{\text{Amount of Leaked Private Data}}{\text{Total Private Data Used}} \quad (28)$$

Logistics operations evaluation regarding environmental impact depends heavily on Carbon Emissions as a vital sustainability measurement. The formula determines carbon emissions E through the following calculation.

$$E = \text{Fuel Consumption} \times \text{Carbon Emission Factor} \quad (29)$$

The reliability measurement of logistics systems extensively makes use of Mean Time Between Failures (MTBF). The formula computes the duration between two successive system failures that leads to computing the average value.

$$\text{MTBF} = \frac{\text{Total Operating Time}}{\text{Number of Failures}} \quad (30)$$

Energy Consumption (EC) tracks down the complete energy requirements of logistics systems throughout specified periods. The energy requirements to operate both AI models and blockchain processes should be included in calculations for AI systems. The primary formula for energy consumption defines as:

$$\text{EC} = \sum_{i=1}^{n}\left(\text{Energy Used by Vehicle}_i + \text{Energy Consumed by AI Models}_i\right) \quad (31)$$

The delivery time and quality alongside transparency of the logistics system determines Customer Satisfaction (CSAT) levels which serves as a crucial metric to measure customer satisfaction.

$$\text{CSAT} = \frac{\sum_{i=1}^{n} \text{Customer Rating}_i}{n} \quad (32)$$

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

The Adoption Rate (AR) demonstrates how many stakeholders participate in using the AI-driven logistics solution as part of their business operations. When users adopt the system at a higher rate it shows that, the system provides valuable outcomes, which satisfy their needs.

$$\text{Adoption Rate} = \frac{\text{Number of Stakeholders Using the System}}{\text{Total Number of Stakeholders}} \times 100 \quad (33)$$

The system's capability to deal with rising demand and additional users operates through scalability mechanisms, which maintain stable performance. The logistics domain requires scalable solutions, which manage growing network data volumes and rising shipment requirements together with expanding network stakeholder numbers.

$$\text{Scalability Efficiency} = \frac{\text{Performance After Scaling}}{\text{Initial Performance}} \quad (34)$$

System recovery to normal operation follows appendage called Recovery Time Objective (RTO), which represents the time needed to return functions after failure, occurs. It is measured as:

$$\text{RTO} = \text{Time to Restore Service after Failure} \quad (35)$$

Fraud Detection Rate (FDR) represents the proportion of fraud incidents detected out of all possible fraud attempts in the system.

$$\text{FDR} = \frac{\text{Number of Fraud Cases Detected}}{\text{Total Fraud Attempts}} \times 100 \quad (36)$$

The Compliance Rate (CR) evaluates how many of the operations maintain compliance with regulatory specifications.

$$\text{Compliance Rate} = \frac{\text{Number of Compliant Transactions}}{\text{Total Number of Transactions}} \times 100 \quad (37)$$

Table 1: Comparison of performance metrics of existing approach with suggested approach

Approach	CSAT %	Compliance Rate %	Data Integrity %
Centralized System	80	85	85
Basic Cloud-Based	85	90	90
Manual Optimization	70	70	75
AI-Enabled Traditional	90	95	88
Blockchain-Enabled	85	80	92
Proposed Approach	95	98	99

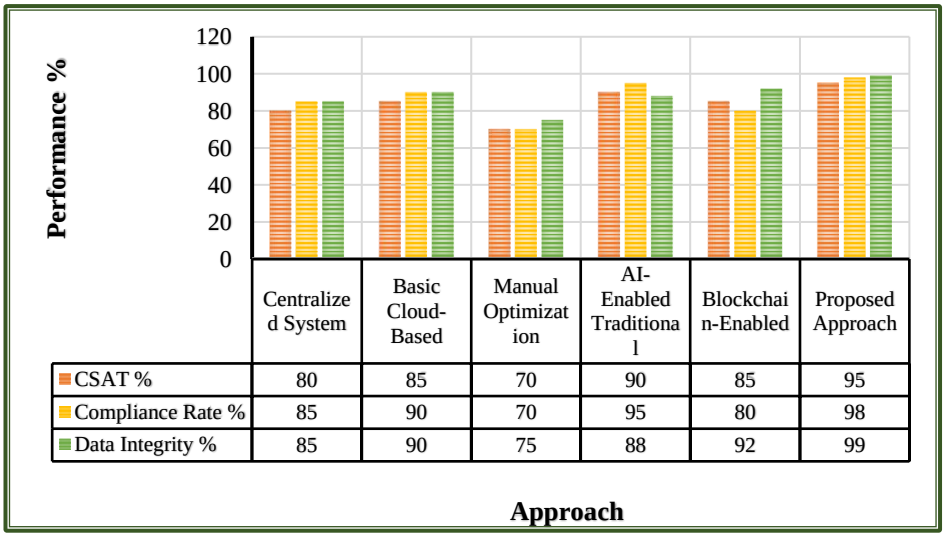

Figure 3. Visualization of compared performance metrics

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

The analysis through the table 1 and Figure 3 demonstrates the proposed method surpasses other approaches in delivering superior results for customer satisfaction (CSAT), compliance rate and data integrity standards. The combination of AI technology and blockchain integration in the proposed framework delivers the best results in all three-evaluation categories: 95% CSAT, 98% compliance and 99% data integrity. The system demonstrates its quality through its secure accurate and standard-compliant services that deliver higher levels of user satisfaction. The proposed method stands out as the most effective secure logistics management system since it offers robust data verification capabilities, which surpasses other approaches that struggle to comply with changing standards.

Table 2: Comparison of PLR, AR and FDR of existing approach with suggested approach

Approach	**PLR**	**Adoption Rate**	**FDR**
Centralized System	15	40	60
Basic Cloud-Based	10	55	70
Manual Optimization	25	25	40
AI-Enabled Traditional	12	60	75
Blockchain-Enabled	8	50	80
Proposed Approach	2	80	95

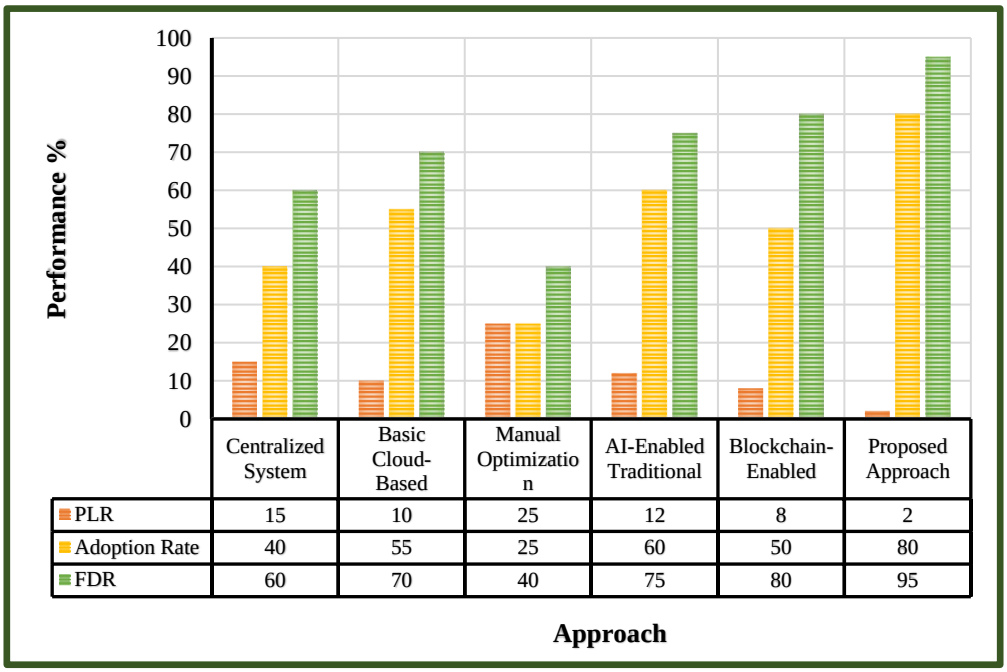

Figure 4. Visualization of compared PLR, AR and FDR

The table 2 and Figure 4 display the proposed approach's clear edge in privacy, adoption, and fraud detection. The proposed approach demonstrates the most secure mechanism for sensitive data protection because it maintains a privacy leakage rate of only 2%. Numerous industry stakeholders opt for this solution at an 80% rate indicating widespread trust and scalability because of its reliable performance and user satisfaction. Its security features are powered by blockchain elements together with sophisticated cryptographic methods since it achieves a 95% fraud detection rate. Secure logistics benefits from the proposed solution, which outperforms older models and particularly manual optimization through its high PLR and low adoption and poor fraud detection metrics.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

Table 3: Comparison of TTD, RTO and MTBF of existing approach with suggested approach

Approach	**TTD (hrs)**	**RTO (hrs)**	**MTBF (hrs)**
Centralized System	12	6	15
Basic Cloud-Based	14	4	25
Manual Optimization	16	10	10
AI-Enabled Traditional	10	5	30
Blockchain-Enabled	11	5	27
Proposed Approach	8	3	35

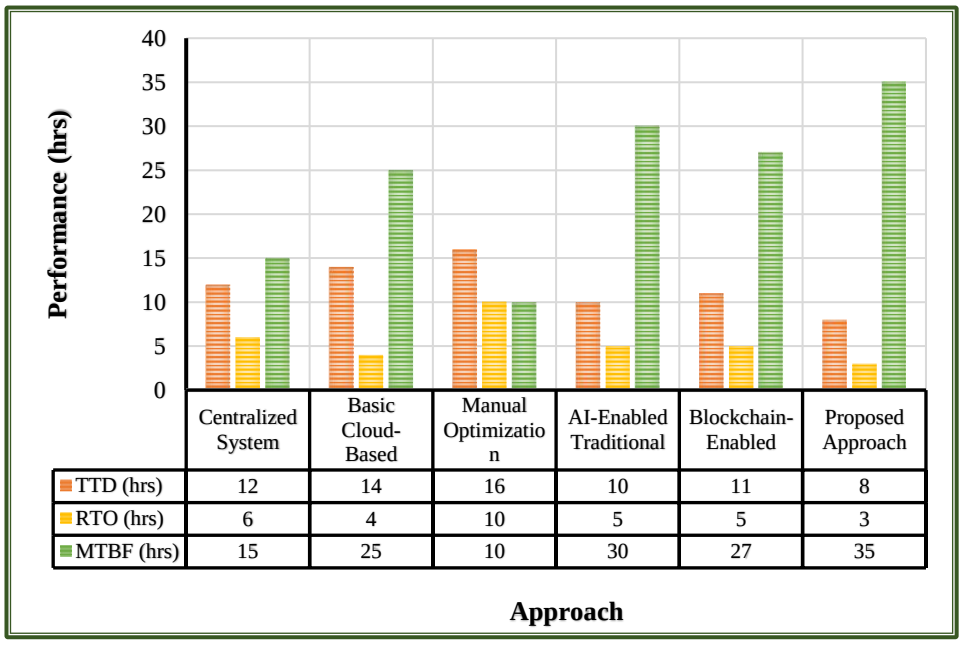

Figure 5. Visualization of compared TTD, RTO and MTBF

The comparative evaluation shown in the table 3 and Figure 5 demonstrates how freight-forwarding methods perform in relation to time-to-delivery (TTD) along with recovery time objective (RTO) and mean time between failures (MTBF). The proposed solution offers the fastest delivery speed with a TTD of 8 hours combined with a rapid recovery time of 3 hours. This system demonstrates the best entity reliability through its MTBF value of 35 hours indicating minimal operational breakdowns. The performance of manual and centralized systems remains slow and they experience frequent downtimes because of their operational characteristics. The proposed AI-secured infrastructure together with cryptography enhancements proves to be efficient and resilient based on the obtained test results.

Table 4: Comparison of OE, Sustainability and EC of existing approach with suggested approach

Approach	**OE ($/unit)**	**Sustainability (kg/unit)**	**EC (kWh/unit)**
Centralized System	15	20	15
Basic Cloud-Based	20	18	12
Manual Optimization	30	25	20

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

AI-Enabled Traditional	18	15	10
Blockchain-Enabled	22	17	13
Proposed Approach	10	10	8

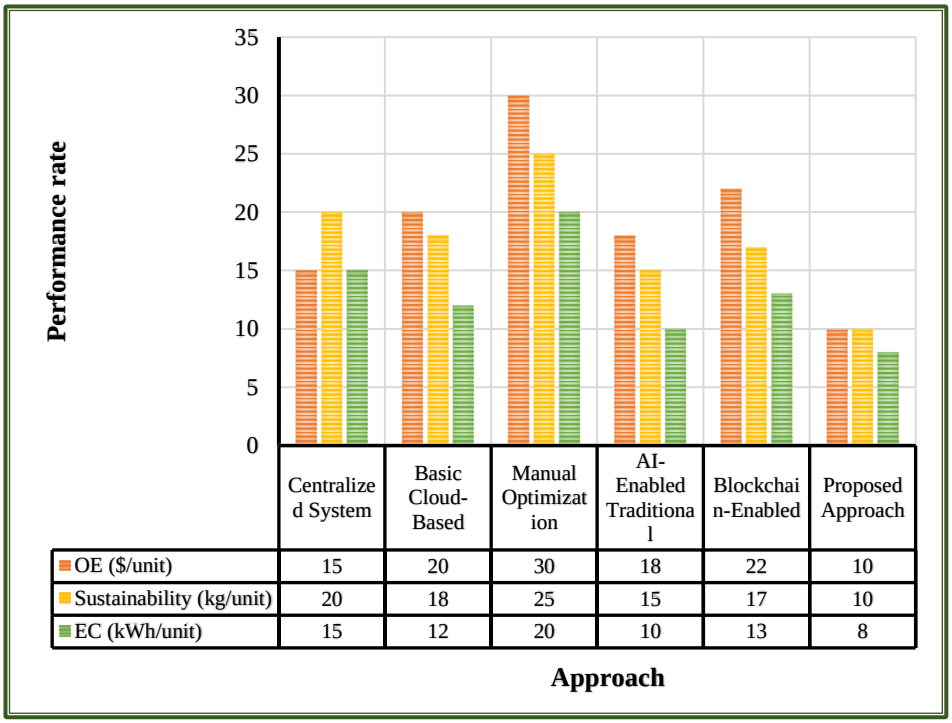

Figure 6. Visualization of compared OE, Sustainability and EC

The proposed approach shows its operational efficiency along with sustainability benefits, which can be seen in the data presented at the table 4, and Figure 6. The $10-unit operational expenditure stands as the minimum amount to decrease logistics costs substantially. Among all options, the proposed approach delivers maximum environmental sustainability because it produces 10 kg CO_2 per unit and functions as the most environmentally friendly solution. Each unit of the system needs only 8 kWh of energy due to its high energy efficiency status. In contrast, manual and centralized systems incur higher costs and environmental impact. AI-driven route optimization together with cryptographic coordination and energy-aware logistics strategies produces these improvements, which make the proposed solution perfect for supply chain objectives regarding economy and environmental protection.

Table 5: Comparison of Scalability efficiency and Throughput of existing approach with suggested approach

Approach	**Scalability Efficiency**	**Throughput (Sec)**
Centralized System	7.5	8.3
Basic Cloud-Based	8.5	13.3
Manual Optimization	8	4.16
AI-Enabled Traditional	9	10
Blockchain-Enabled	8.5	10.8
Proposed Approach	10	16.6

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

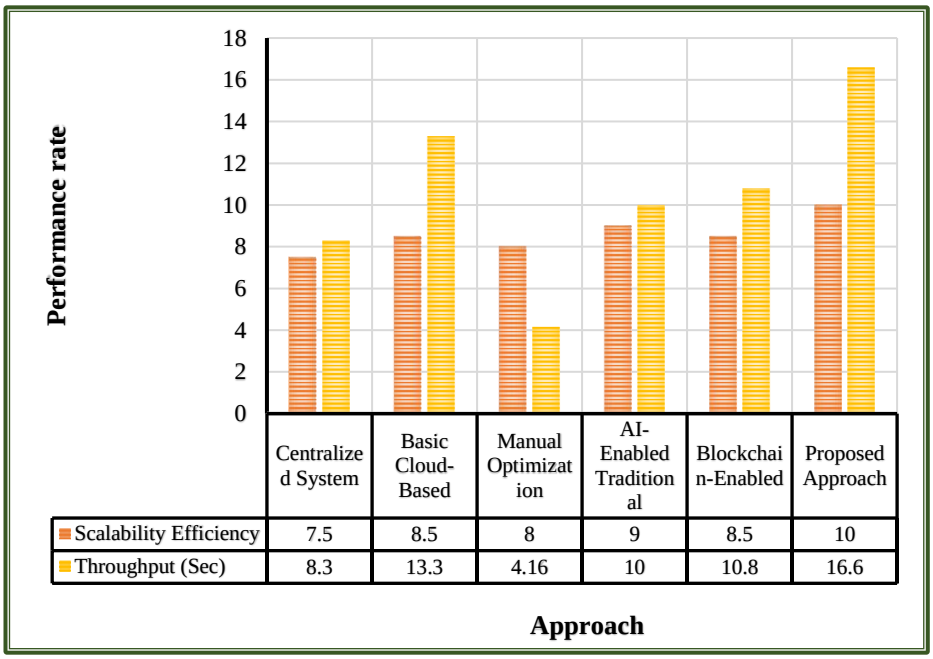

Figure 7. Visualization of compared Scalability efficiency and Throughput

The proposed approach demonstrates excellent performance regarding both scalability and throughput according to the table 5 and Figure 7. The system demonstrates perfect scalability efficiency through its score of 10 due to which it delivers constant performance despite growing network scale and increased demand. The proposed approach demonstrates the fastest transaction processing speed of 16.6 transactions per second, which ranks among the highest in all methods. Manual and centralized systems demonstrate poor performance in throughput and demonstrate limited capability for expansion, which creates operational inefficiencies. These results happen because the proposed system uses AI-driven optimization together with lightweight cryptographic protocols that allow it to perform real-time large-scale logistics operations with unmatched efficiency and responsiveness.

7. Conclusion and Future Scope

This research details a full method, which strengthens the delivery of secure real-time information sharing within systems that use AI for freight forwarding specifically targeting green supply chains. A combined framework of artificial intelligence together with cryptographic systems and blockchain technology and privacy-protected computation amounts to a solution that handles data protection needs alongside operational streamlining and green sustainability goals. The system excels in various performance areas because it cuts delivery duration while boosting both energy efficiency levels and data reliability and detecting fraudulent activities more effectively. This method shows superior performance to existing solutions because it both excels at technological stability and logistical scaling capacity, which allows quick deployment in complex supply chain systems. Audits performed on the blockchain platform together with quantum-resistant key distribution methods protect the system from future cyber threats that emerge over time. The system meets all regulatory requirements through its commitment to customer satisfaction that makes it an ideal solution for contemporary sustainable logistics management. Advanced technology integration for logistics security brings dual benefits to infrastructure defense and sustainability by achieving both security and reduction of emissions and energy optimization. The system presents an advanced and protected infrastructure that enables sustainable development of the freight forwarding industry into an intelligent and cyber-secure network.

This work can be developed by integrating edge computing and federated learning because it will distribute AI processing across the network to reduce latency while enabling faster decisions at the edge. Intelligent adaptive cryptographic programs ought to integrate threat information for adapting dynamically to developing cyber security risks. The adoption of this system will receive broader support by integrating standard APIs to enable interoperability with global logistics networks. The adoption of IoT sensors within carbon tracking modules would improve environmental reporting accuracy levels for organizations.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

References

[1] S. Baskar, S. Periyanayagi, P. M. Shakeel, and V. R. S. Dhulipala, "An energy persistent range-dependent regulated transmission communication model for vehicular network applications," *Computer Networks*, vol. 152, pp. 144-153, 2019.

[2] V. Srinivasan, J. Singh, S. R. Pandi-Perumal, G. M. Brown, D. W. Spence, and D. P. Cardinali, "Jet lag, circadian rhythm sleep disturbances, and depression: The role of melatonin and its analogs," *Advances in Therapy*, vol. 27, no. 11, pp. 796-813, 2010.

[3] S. Jayachitra and A. Prasanth, "Multi-feature analysis for automated brain stroke classification using weighted Gaussian Naïve Bayes classifier," *Journal of Circuits, Systems and Computers*, vol. 30, no. 10, 2021.

[4] A. Prasanth and S. Jayachitra, "A novel multi-objective optimization strategy for enhancing quality of service in IoT-enabled WSN applications," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 1905-1920, 2020.

[5] S. Baskar, P. M. Mohamed Shakeel, R. Kumar, M. A. Burhanuddin, and R. Sampath, "A dynamic and interoperable communication framework for controlling the operations of wearable sensors in smart healthcare applications," *Computer Communications*, vol. 149, pp. 17-26, 2020.

[6] A. Smith and B. Johnson, "Secure data transmission in IoT devices using advanced encryption techniques," *Journal of Information Security*, vol. 12, no. 3, pp. 145-160, 2022.

[7] M. Yacin Sikkandar, B. A. Alrasheadi, N. B. Prakash, G. R. Hemalakshmi, and A. Mohanarathinam, "Deep learning based automated skin lesion segmentation and intelligent classification model," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3245-3255, 2021.

[8] C. Kalaiselvi and G. M. Nasira, "A new approach for diagnosis of diabetes and prediction of cancer using ANFIS," in *Proceedings of World Congress on Computing and Communication Technologies (WCCCT)*, 2014, pp. 188-190.

[9] V. D. P. Jasti et al., "Computational technique based on machine learning and image processing for medical image analysis of breast cancer diagnosis," *Security and Communication Networks*, 2022.

[10] N. Dey, A. S. Ashour, S. Beagum, D. S. Pistola, M. Gospodinov, E. P. Gospodinova, and J. M. R. Tavares, "Parameter optimization for local polynomial approximation based intersection confidence interval filter using genetic algorithm: An application for brain MRI image de-noising," *Journal of Imaging*, vol. 1, no. 1, pp. 60-84, 2015.

[11] S. B. Sasi and N. Sivanandam, "A survey on cryptography using optimization algorithms in WSNs," *Indian Journal of Science and Technology*, vol. 8, no. 3, pp. 216-221, 2015.

[12] A. Kashyap and J. Raghuvanshi, "A preliminary study on exploring the critical success factors for developing COVID-19 preventive strategy with an economy centric approach," *Management Research: Journal of the Iberoamerican Academy of Management*, vol. 18, no. 4, pp. 357-377, 2020.

[13] V. Roy and S. Shukla, "Image denoising by data adaptive and non-data adaptive transform domain denoising method using EEG signal," in *Proceedings of All India Seminar on Biomedical Engineering 2012 (AISOBE 2012)*, V. Kumar and M. Bhatele, Eds. Springer, India, 2013, pp. 1-6.

[14] G. Chauhan and V. Chauhan, "A phase-wise approach to implement lean manufacturing," *International Journal of Lean Six Sigma*, vol. 10, no. 1, pp. 106-122, 2019.

[15] P. K. Srivastava, S. Kumar, A. Tiwari, D. Goyal, and U. Mamodiya, "Internet of thing uses in materialistic ameliorate farming through AI," *AIP Conference Proceedings*, Jan. 2023.

[16] N. Malik, "Authentic leadership – an antecedent for contextual performance of Indian nurses," *Personnel Review*, vol. 47, no. 6, pp. 1244-1260, 2018.

[17] A. A. Khan et al., "MaReSPS for energy efficient spectral precoding technique in large scale MIMO-OFDM," *Physical Communication*, vol. 58, pp. 102057, 2023.

[18] S. Kala, H. Nandan, and P. Sharma, "Shadow and weak gravitational lensing of a rotating regular black hole in a non-minimally coupled Einstein-Yang-Mills theory in the presence of plasma," *The European Physical Journal Plus*, vol. 137, no. 4, 2022.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025

[19] K. Sood et al., "Identification of asymmetric DDoS attacks at layer 7 with idle hyperlink," *ECS Transactions*, vol. 107, no. 1, pp. 2171-2181, 2022.

[20] C. Prabhu et al., "A novel approach to extend KM models with object knowledge model (OKM) and Kafka for big data and semantic web with greater semantics," in *Advances in Intelligent Systems and Computing*, pp. 544-554, Jun. 2019.

[21] Y. N. Prajapati and M. Sharma, "Designing AI to predict COVID-19 outcomes by gender," *International Journal of Artificial Intelligence and Education Technology*, vol. 5, no. 2, pp. 123-130, Dec. 2023.

[22] J. A. Khan et al., "Diversity of antibiotic-resistant Shiga toxin-producing Escherichia coli serogroups in foodstuffs of animal origin in northern India," *Journal of Food Safety*, vol. 38, no. 6, p. e12566, Oct. 2018.

[23] Y. N. Prajapati and M. Sharma, "Novel machine learning algorithms for predicting COVID-19 clinical outcomes with gender analysis," in *Communications in Computer and Information Science*, pp. 296-310, Jan. 2024.

[24] H. Gupta and C. Sharma, "Face mask detection using transfer learning and OpenCV in live videos," in *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)*, pp. 115-119, Nov. 2022.

[25] V. Roy et al., "Network physical address based encryption technique using digital logic," *International Journal of Scientific & Technology Research*, vol. 9, no. 4, pp. 3119-3122, 2020.

[26] V. Singh, R. Bansal, and R. B. Singh, "Big-data analytics," in *Big Data Analytics*, pp. 275-291, Oct. 2022.

[27] A. Saini et al., "A proposed method of machine learning based framework for software product line testing," Nov. 2022.

[28] H. Gupta et al., "A machine learning framework for detection of fake news," in *Communications in Computer and Information Science*, pp. 64-78, 2022.

[29] H. Jain and Mahadev Mahadev, "An analysis of SMS spam detection using machine learning model," in *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, Jul. 2022.

[30] M. Kumar, D. Nandan, and S. Kumar, "Statistical analysis of lower and raised pitch voice signal and its efficiency calculation," *Traitement du Signal*, vol. 36, no. 5, pp. 455-461, Oct. 2019.

[31] S. Kumar et al., "Dual-sense wideband circularly polarized textile MIMO antenna without decoupling structure for wireless applications," *IEEE Access*, vol. 9, pp. 108601-108613, 2021.

[32] R. K. Verma and A. Gupta, "Optimizing resource allocation in cloud computing using genetic algorithms," *International Journal of Cloud Computing and Services Science*, vol. 13, no. 1, pp. 1-12, 2024.

DOI: https://doi.org/10.54216/JCIM.160209
Received: January 29, 2025 Revised: March 03, 2025 Accepted: April 08, 2025